Bundesamt
für Sicherheit in der
Informationstechnik

IT-Grundschutz im Cyber-Raum

Bonn, 20.05.2015

Dr. Hartmut Isselhorst

Bundesamt
für Sicherheit in der
Informationstechnik

Cyber-Sicherheitslage

Ursachen → Wirkungen

Exploit-Kits nutzen vermehrt 0-Day-Schwach-stellen

1,6% der Spam-Mails enthalten **Malware**

noch **6%** **Windows XP** im Einsatz (unsupportet)

Ca. **340 Mio. Schad-programme** für Windows

Ca. 1150 Botnetze weltweit, davon mehr als 1 Mio. Rechner in D

11% aller Nutzer: **ungepatchte Systeme**

tägl. ca. 2 neue kritische Schwach-stellen in 13 wichtigen Produkten

DDoS-Angriffe: Buy/rent a Bot: 30-70 $/Tag

0-Day-Schwachstelle Deaktivierung des Programmes erforderlich

Drive-by-Exploits: In D allein 3% aller Webseiten verseucht

Hacktivismus zunehmend DDoS-Angriffe auf **KRITIS-Untern. und Behörden**

1,1 Milo. verseuchte Web-Seiten

Aktuelle Bedrohung Schwach-stellen sehr hoch

Kosten nach DDOS-Angriff über 40.000€ für KMU

Gezielte Cyber-spionage durch APT-Angriffe

133 DDoS-Angriffe pro Tag

Ca. 2500% Anstieg im letzten Jahr im mobilen Umfeld

Identitäts-diebstahl: Clients: **16Mio/18Mio** eBay-Server: **145 Mio**

Eldorado Cyber-Raum

Goldgräberstimmung bei Cyber-Kriminellen

Eldorado Cyber-Raum

Cyber-(T)raum für Kriminelle

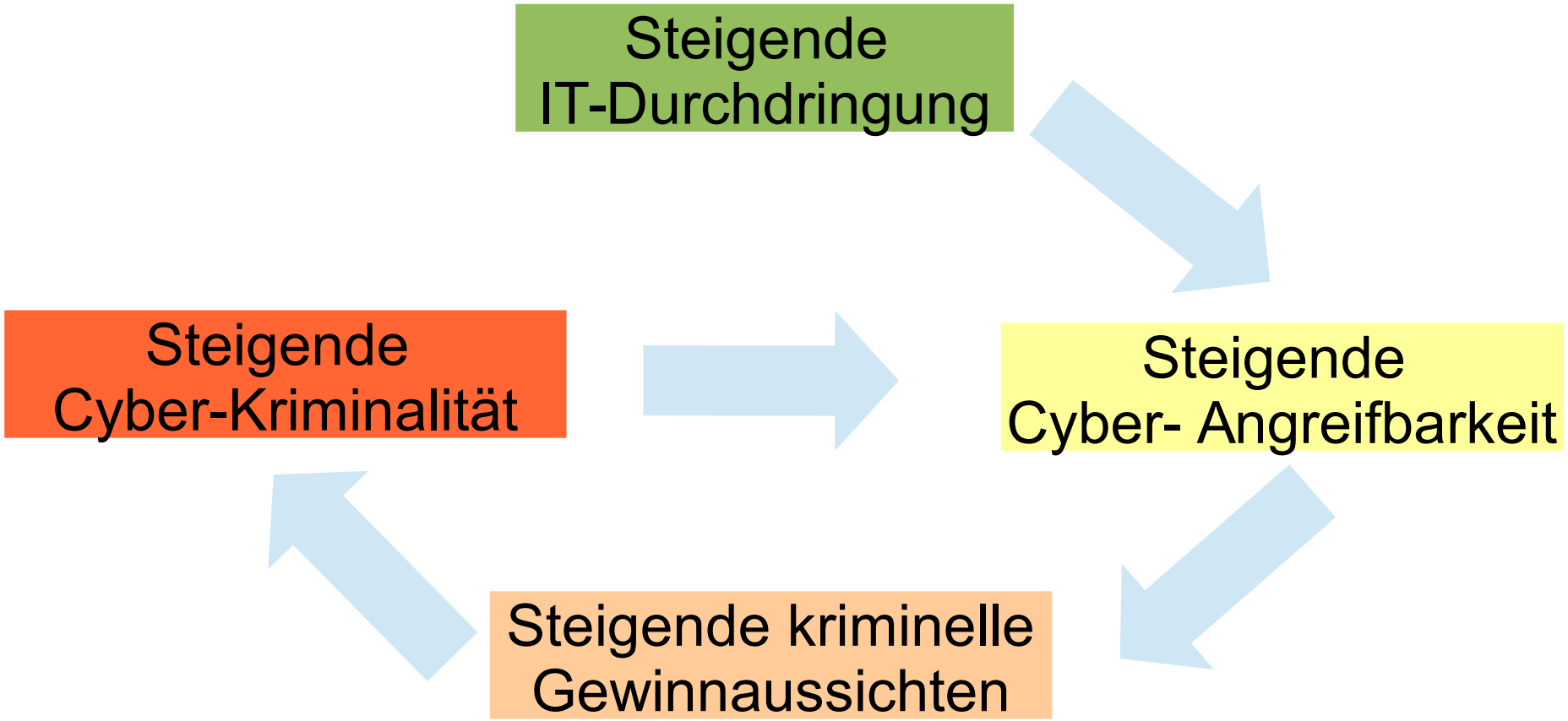
- Rahmenbedingungen
  - Internet-Anonymität = sehr geringes Entdeckungsrisiko
  - Kein „Vor-Ort-Risiko“, Angriff aus der Internet-Ferne
  - Gleichzeitiger Angriff auf zahlreiche Opfer
  - Massenhaft unzureichend geschützte Opfer
  - Billige Grundausstattung < 1000€
  - Sehr preiswerte Tatwerkzeuge < 100€
    (Malware, Spam, DDoS, Bots, …)
  - Anonyme Zahlungsmittel
  - Permanenter Nachschub an Software-Schwachstellen

Eldorado Cyber-Raum

Cyber-(T)raum für Kriminelle

- Folgen
  - Arbeitsteilige industrielle Cyber-Kriminalität
  - 350.000.000 klassische Schadprogramme weltweit
  - 4.500.000 „mobile“ Malware weltweit
  - Extrem schnell agierende Cyber-Kriminelle
  - 1.200 Botnetze
  - Millionen gestohlener Identitäten in Deutschland
  - > 65.000 DDoS-Angriffe p.a. in Deutschland
  - 1/3 der Unternehmen erlebten Cyber-Attacken in den letzten drei Jahren

Cyber-Teufelskreis



Durchbrechen des Cyber-Teufelskreises

Strategien für Cyber-Sicherheit

- **Risiko für Täter erhöhen**
  - Verstärkte polizeiliche Aktivitäten, internationale Kooperation
- **Gewinnerwartung bei Cyber-Angriffen schmälern**
  - Sicherheitsniveau in der Breite erhöhen
  - Good Practice, Erfahrungsaustausch, Kooperation

- **Aktionsfreiräume der Täter verkleinern**
  - Zeitraum des unentdeckten Angriffs verkürzen
  - Paradigmenwechsel Prävention, *Detektion*, Reaktion

- **„Cyber-Diebstahlsperre“, Regulierung**
  - IT-Sicherheitsgesetz (Änderungen TMG, TKG, KRITIS)

Durchbrechen des Cyber-Teufelskreises
BSI-Ansätze

Strategien für Cyber-Sicherheit

- **Risiko für Täter erhöhen**
  - Verstärkte polizeiliche Aktivitäten, internationale Kooperation
- **Gewinnerwartung bei Cyber-Angriffen schmälern**
  - Sicherheitsniveau in der Breite erhöhen
  - Good Practice, Erfahrungsaustausch, Kooperation
- **Aktionsfreiräume der Täter verkleinern**
  - Zeitraum des unentdeckten Angriffs verkürzen
  - Paradigmenwechsel Prävention, *Detektion*, Reaktion
- **„Cyber-Diebstahlsperre" Regulierung**
  - IT-Sicherheitsg[illegible]en TMG, TKG, KRITIS)

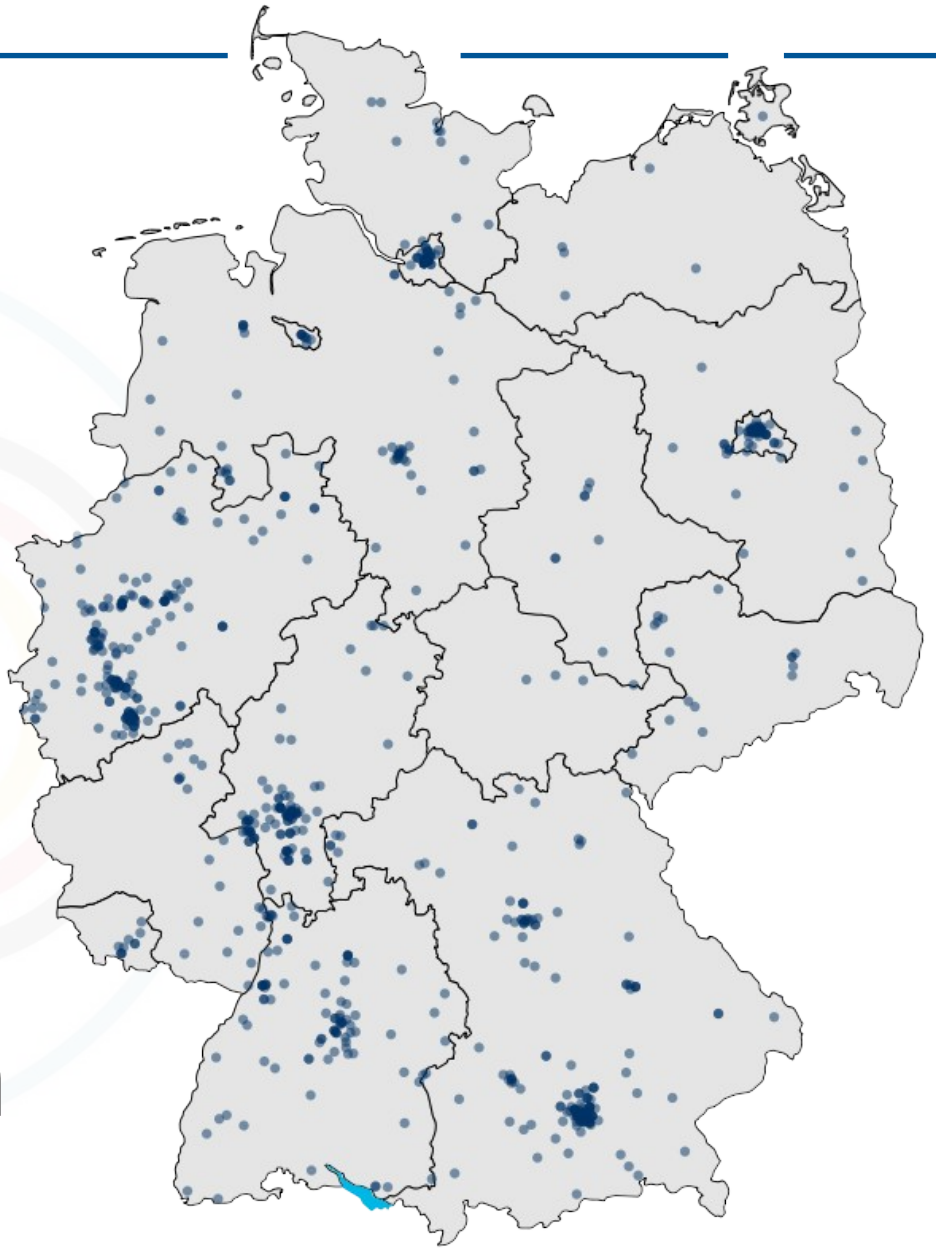
Bundesamt
für Sicherheit in der
Informationstechnik

Allianz für Cyber-Sicherheit

Stand: 04.05.2015

1236

Unternehmen



80 Partner

38 Multiplikatoren

Durchbrechen des Cyber-Teufelskreises
BSI-Ansätze

Strategien für Cyber-Sicherheit

- **Risiko für Täter erhöhen**
  - Verstärkte polizeiliche Aktivitäten, internationale Kooperation
- **Gewinnerwartung bei Cyber-Angriffen schmälern**
  - Sicherheitsniveau in der Breite erhöhen
  - Good Practice, Erfahrungsaustausch, Kooperation
- **Aktionsfreiräume der Täter verkleinern**
  - Zeitraum des unentdeckten Angriffs verkürzen
  - Paradigmenwechsel Prävention, *Detektion*, Reaktion
- **„Cyber-Diebstahlsperre“, Regulierung**
  - IT-Sicherheitsgesetz (Änderungen TMG, TKG, KRITIS)

IT-Grundschutz

IT-Grundschutz im Cyber-Raum

Sicherheitsniveau in der Breite erhöhen

Anforderungen an den IT-Grundschutz im Cyber-Raum

- Zeitnahe Adaption realer/neuer (Cyber-)Gefährdungen
- Schnellere Bereitstellung von Inhalten/Empfehlungen
- Zielgruppe erweitern um kleine/mittelständische Institutionen
- Integration von industrieller IT
- Skalierbarkeit
  - Vorgehensweise, Aufwand, Schutzbedarf (normal, hoch)
- Paradigmenwechsel:
  - Nicht alle Angriffe lassen sich präventiv beherrschen
  - -> Integration von Detektionsprozessen
- Betonung der Risikomanagement-Prozesse
- Kompatibilität zu ISO 27001

Modernisierung des IT-Grundschutzes

- Breite Beteiligung aller Zielgruppen (2014/2015) Eingebunden wurden
  - IT-Grundschutz-Anwender
    - Verwaltung (Bund, Länder, Kommunen)
    - Wirtschaft (Großunternehmen, KMU)
  - Auditoren
  - IT-Sicherheitsberater
  - Hersteller von IT-Grundschutz-Tools
- Hohe Zustimmung zu Modernisierungsansätzen

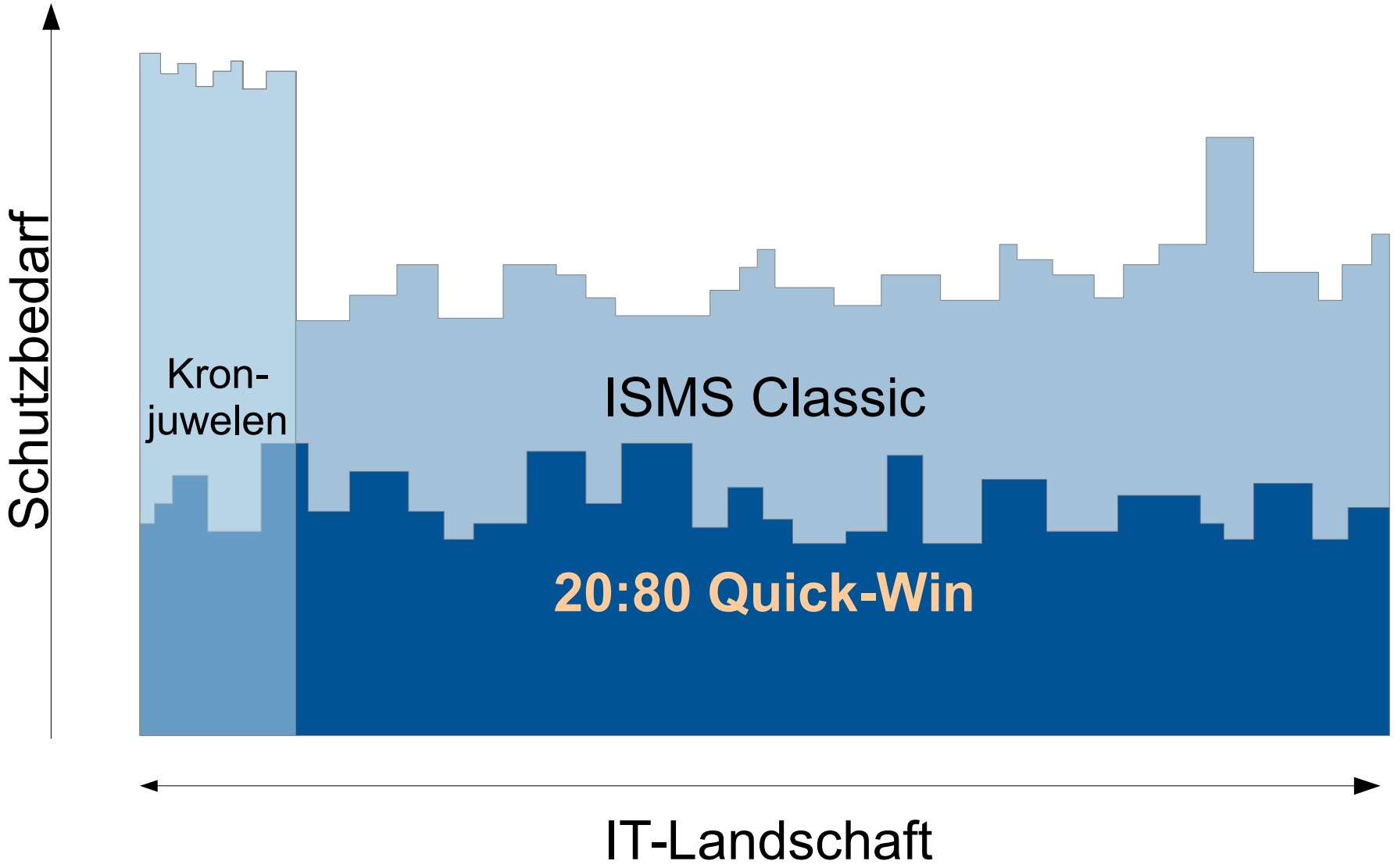
Design-Entscheidungen

Skalierbarkeit Schutzbedarf

Dreistufige Maßnahmensortierung:

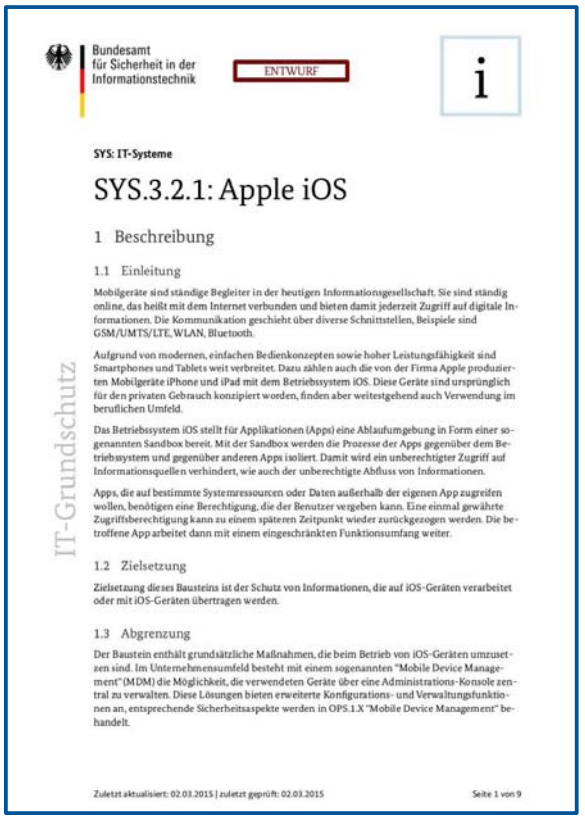
- **Erstmaßnahmen**
  - die „allerwichtigsten“ Maßnahmen
  - sollten prioritär umgesetzt werden (-> 20:80-Vorgehensweise)
- **Basismaßnahmen**
  - erzeugen zusammen mit den Erstmaßnahmen eine angemessene IT-Sicherheit für den „Normalfall“
- **Hochschutz-Maßnahmen**
  - Naheliegende Maßnahmen zum erhöhten Schutz von Vertraulichkeit (C), Integrität (I) und/oder Verfügbarkeit (A)

Skalierbarkeit Vorgehensweisen



Aufbau der Bausteine
Zielgruppe: CISO

- **Umfang: ca. 10 Seiten!**
- Beschreibung
  - Einleitung
  - Zielsetzung
  - Abgrenzung
- Gefährdungslage
- **Maßnahmen als Anforderungen**
  - Erstmaßnahmen
  - Basismaßnahmen
  - Maßnahmen für erhöhten Schutzbedarf
- Referenzen auf weiterführende Informationen
- Anlage: Kreuzreferenztabelle zu Elementaren Gefährdungen



Bundesamt
für Sicherheit in der
Informationstechnik

ENTWURF

i

SYS: IT-Systeme

SYS.3.2.1: Apple iOS

1 Beschreibung

1.1 Einleitung

Mobilgeräte sind ständige Begleiter in der heutigen Informationsgesellschaft. Sie sind ständig online, das heißt mit dem Internet verbunden und bieten damit jederzeit Zugriff auf digitale Informationen. Die Kommunikation geschieht über diverse Schnittstellen, Beispiele sind GSM/UMTS/LTE, WLAN, Bluetooth.

Aufgrund von modernen, einfachen Bedienkonzepten sowie hoher Leistungsfähigkeit sind Smartphones und Tablets weit verbreitet. Dazu zählen auch die von der Firma Apple produzierten Mobilgeräte iPhone und iPad mit dem Betriebssystem iOS. Diese Geräte sind ursprünglich für den privaten Gebrauch konzipiert worden, finden aber weitestgehend auch Verwendung im beruflichen Umfeld.

Das Betriebssystem iOS stellt für Applikationen (Apps) eine Ablaufumgebung in Form einer sogenannten Sandbox bereit. Mit der Sandbox werden die Prozesse der Apps gegenüber dem Betriebssystem und gegenüber anderen Apps isoliert. Damit wird ein unberechtigter Zugriff auf Informationsquellen verhindert, wie auch der unberechtigte Abfluss von Informationen.

Apps, die auf bestimmte Systemressourcen oder Daten außerhalb der eigenen App zugreifen wollen, benötigen eine Berechtigung, die der Benutzer vergeben kann. Eine einmal gewährte Zugriffsberechtigung kann zu einem späteren Zeitpunkt wieder zurückgezogen werden. Die betroffene App arbeitet dann mit einem eingeschränkten Funktionsumfang weiter.

1.2 Zielsetzung

Zielsetzung dieses Bausteins ist der Schutz von Informationen, die auf iOS-Geräten verarbeitet oder mit iOS-Geräten übertragen werden.

1.3 Abgrenzung

Der Baustein enthält grundsätzliche Maßnahmen, die beim Betrieb von iOS-Geräten umzusetzen sind. Im Unternehmensumfeld besteht mit einem sogenannten "Mobile Device Management" (MDM) die Möglichkeit, die verwendeten Geräte über eine Administrations-Konsole zentral zu verwalten. Diese Lösungen bieten erweiterte Konfigurations- und Verwaltungsfunktionen an, entsprechende Sicherheitsaspekte werden in OPS.1.X "Mobile Device Management" behandelt.

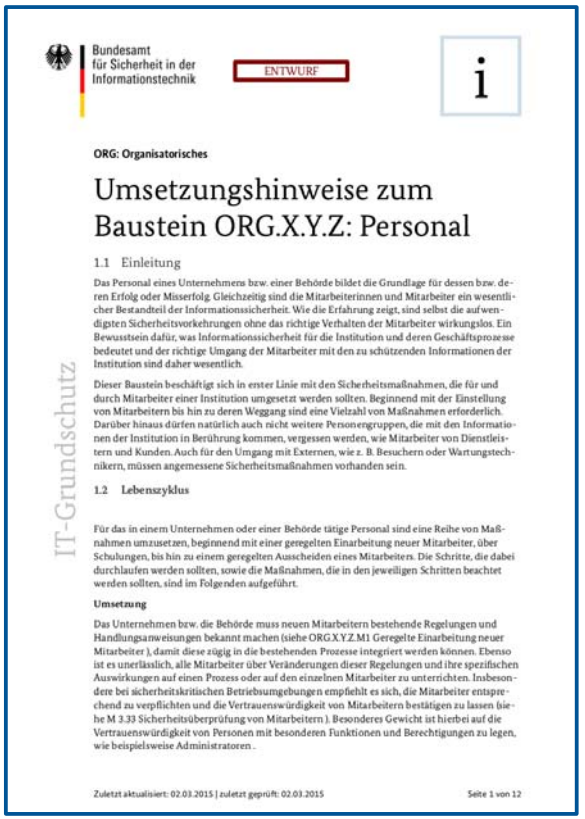
IT-Grundschutz

Zuletzt aktualisiert: 02.03.2015 | zuletzt geprüft: 02.03.2015

Seite 1 von 9

Umsetzungshinweise
Zielgruppe: Umsetzer der Maßnahmen

- **Umfang: beliebig**
- Gliederung lehnt sich an Bausteine an
- Beschreibung
  - Einleitung
  - Lebenszyklus
  - Zielsetzung
- **Maßnahmen als Umsetzungshilfen**
  - Erstmaßnahmen
  - Basismaßnahmen
  - Maßnahmen für erhöhten Schutzbedarf
- Referenzen auf weiterführende Informationen
  - Alte IT-GS-Bausteine, Studien, Herstellerdokumentation etc.


Bundesamt
für Sicherheit in der
Informationstechnik

ENTWURF

i

ORG: Organisatorisches

Umsetzungshinweise zum
Baustein ORG.X.Y.Z: Personal

1.1 Einleitung

Das Personal eines Unternehmens bzw. einer Behörde bildet die Grundlage für dessen bzw. deren Erfolg oder Misserfolg. Gleichzeitig sind die Mitarbeiterinnen und Mitarbeiter ein wesentlicher Bestandteil der Informationssicherheit. Wie die Erfahrung zeigt, sind selbst die aufwendigsten Sicherheitsvorkehrungen ohne das richtige Verhalten der Mitarbeiter wirkungslos. Ein Bewusstsein dafür, was Informationssicherheit für die Institution und deren Geschäftsprozesse bedeutet und der richtige Umgang der Mitarbeiter mit den zu schützenden Informationen der Institution sind daher wesentlich.

Dieser Baustein beschäftigt sich in erster Linie mit den Sicherheitsmaßnahmen, die für und durch Mitarbeiter einer Institution umgesetzt werden sollten. Beginnend mit der Einstellung von Mitarbeitern bis hin zu deren Weggang sind eine Vielzahl von Maßnahmen erforderlich. Darüber hinaus dürfen natürlich auch nicht weitere Personengruppen, die mit den Informationen der Institution in Berührung kommen, vergessen werden, wie Mitarbeiter von Dienstleistern und Kunden. Auch für den Umgang mit Externen, wie z. B. Besuchern oder Wartungstechnikern, müssen angemessene Sicherheitsmaßnahmen vorhanden sein.

1.2 Lebenszyklus

Für das in einem Unternehmen oder einer Behörde tätige Personal sind eine Reihe von Maßnahmen umzusetzen, beginnend mit einer geregelten Einarbeitung neuer Mitarbeiter, über Schulungen, bis hin zu einem geregelten Ausscheiden eines Mitarbeiters. Die Schritte, die dabei durchlaufen werden sollten, sowie die Maßnahmen, die in den jeweiligen Schritten beachtet werden sollten, sind im Folgenden aufgeführt.

Umsetzung

Das Unternehmen bzw. die Behörde muss neuen Mitarbeitern bestehende Regelungen und Handlungsanweisungen bekannt machen (siehe ORG.X.Y.Z.M1 Geregelte Einarbeitung neuer Mitarbeiter), damit diese zügig in die bestehenden Prozesse integriert werden können. Ebenso ist es unerlässlich, alle Mitarbeiter über Veränderungen dieser Regelungen und ihre spezifischen Auswirkungen auf einen Prozess oder auf den einzelnen Mitarbeiter zu unterrichten. Insbesondere bei sicherheitskritischen Betriebsumgebungen empfiehlt es sich, die Mitarbeiter entsprechend zu verpflichten und die Vertrauenswürdigkeit von Mitarbeitern bestätigen zu lassen (siehe M 3.33 Sicherheitsüberprüfung von Mitarbeitern). Besonderes Gewicht ist hierbei auf die Vertrauenswürdigkeit von Personen mit besonderen Funktionen und Berechtigungen zu legen, wie beispielsweise Administratoren.

Zuletzt aktualisiert: 02.03.2015 | zuletzt geprüft: 02.03.2015

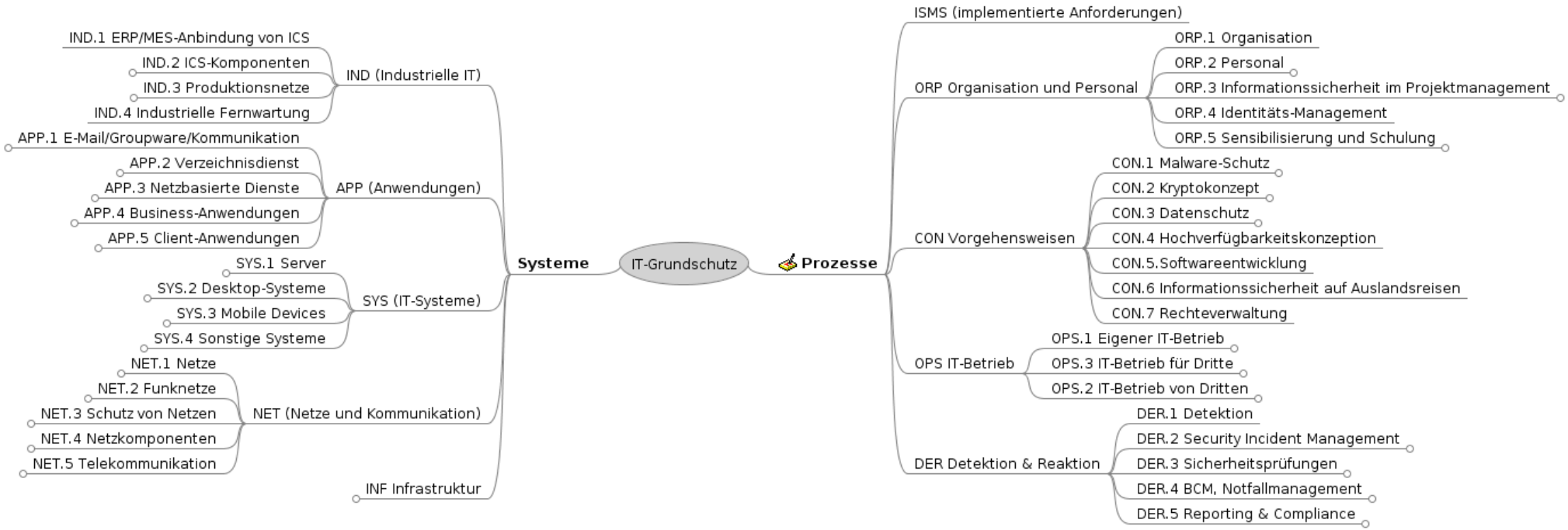
Seite 1 von 12

IT-Grundschutz

Baustein-Struktur

Systeme

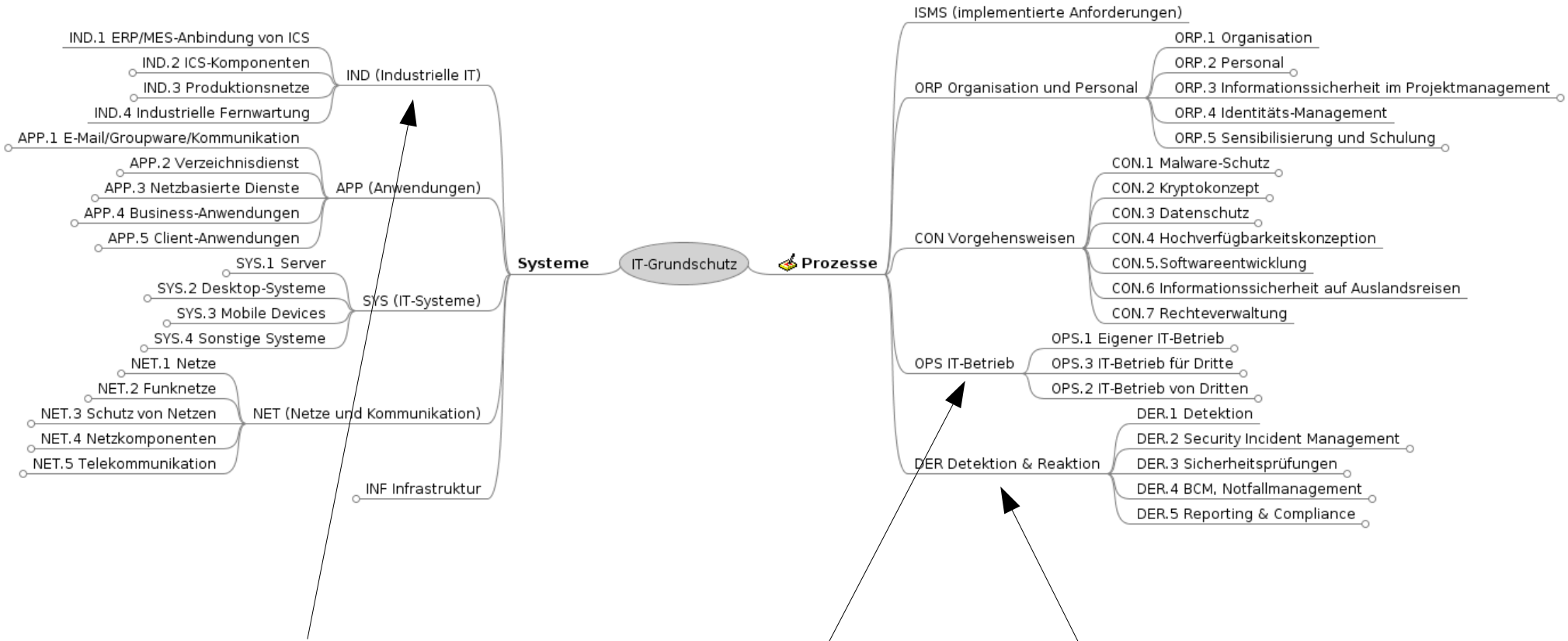
Prozesse



Baustein-Struktur

Systeme

Prozesse



Industrielle IT

IT-Betrieb

Detektion

IT-Grundschutz-Profile

- Profile beziehen sich auf typische IT-Szenarien
  - Beispiele: Kommunalbehörde, Krankenhaus, Cloud-Anbieter
- Profile bestehen aus:
  - Ausgewählter Vorgehensweise
  - Ausgewählten Bausteinen
  - Ausgewählten Maßnahmen in den Bausteinen
  - Ggf. ergänzenden Maßnahmen

- Profile bilden damit eine pauschalisierte Vorauswahl von IT-Grundschutz-Elementen mit spezifischen Ergänzungen
- Profile werden in der Regel durch Dritte (Verbände, Branchen,...), nicht durch das BSI erstellt

Zeitlicher Überblick

- Nächste klassische Ergänzungslieferung Ende 2015

- Weiterhin Einbeziehung der Stakeholder
- Bereitstellung modernisierter / neuer Komponenten ab Anfang 2016
  - Vorgehensweisen
  - Bausteine
- Migration marktgängiger Tools 2016
- Umstellung der IT-Grundschutz-Zertifizierung in 2017

IT-Sicherheitsgesetz

IT-Sicherheitsgesetz

§ 8a (1)

Betreiber Kritischer Infrastrukturen sind **verpflichtet**, …
angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei ist der **Stand der Technik zu berücksichtigen**.

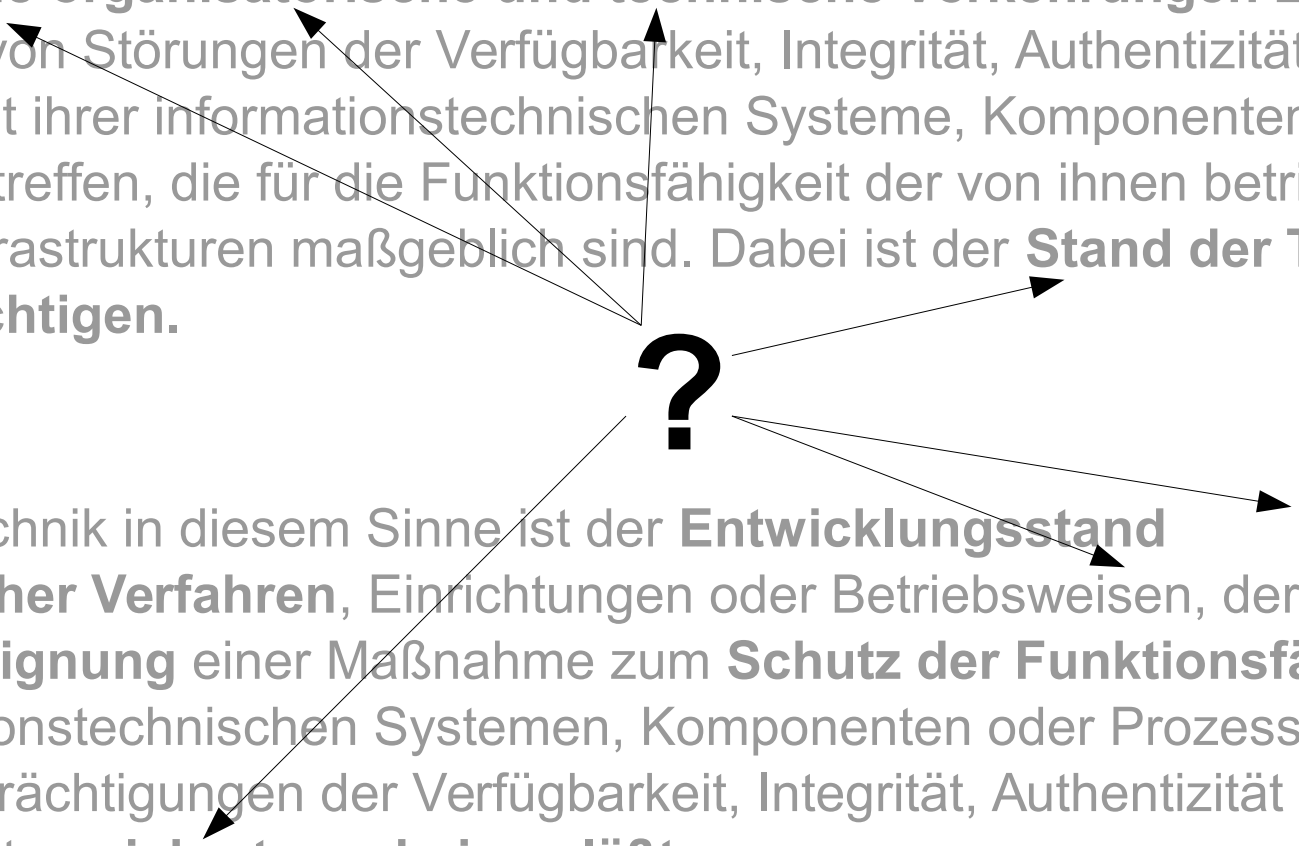
Begründung:

Stand der Technik in diesem Sinne ist der **Entwicklungsstand fortschrittlicher Verfahren**, Einrichtungen oder Betriebsweisen, der die **praktische Eignung** einer Maßnahme zum **Schutz der Funktionsfähigkeit** von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit **gesichert erscheinen läßt**.

IT-Sicherheitsgesetz

§ 8a (1)

Betreiber Kritischer Infrastrukturen sind **verpflichtet, …**
angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei ist der **Stand der Technik zu berücksichtigen.**



Begründung:

Stand der Technik in diesem Sinne ist der **Entwicklungsstand fortschrittlicher Verfahren**, Einrichtungen oder Betriebsweisen, der die **praktische Eignung** einer Maßnahme zum **Schutz der Funktionsfähigkeit** von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit **gesichert erscheinen läßt**.

IT-Sicherheitsgesetz

§ 8a (1)

Betreiber Kritischer Infrastrukturen sind verpflichtet, …
angemessene organisatorische und technische Vorkehrungen zur
Ve … und
Ve … oder
Pr … ebenen
Kr … chnik zu
be …

Be …
St … ttlicher
Ve … hung
ei …
informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen läßt.

Modernisierter IT-Grundschutz nicht als Vorgabe, sondern als

Orientierungshilfe

für

- **Stand der Technik**
- **branchenspezifische Sicherheitsstandards**

Kontakt

Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Dr. Hartmut Isselhorst
Godesberger Allee 185-189
53175 Bonn

Tel.: +49 (0)228 99 9582-5100

hartmut.isselhorst@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de